(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **61063128 A**

(43) Date of publication of application: **01 . 04 . 86**

(51) Int. Cl **H04L 9/02**

(21) Application number: **59185186**

(22) Date of filing: **04 . 09 . 84**

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT>**

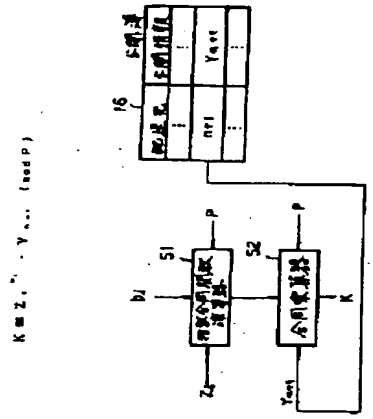
(72) Inventor: **OKAMOTO TATSUAKI**
SHIRAISHI AKIRA

(54) CIPHERING KEY DISTRIBUTION SYSTEM

(57) Abstract:

PURPOSE: To distribute effectively a key from one distribution sender to plural distribution destinations under the recognition of the both the parties by allowing each key distribution destination to use reception information and secret information possessed by the own destination so as to obtain a key from the information generated by key distribution sender through the use of a random number and public information.

CONSTITUTION: The distribution sender generate information transferred to each distribution destination (i) by using the generated random number and the information transmitted to each distribution destination and system public information and transmits the result to each distribution destination. Then each distribution destination (i) (i=1, 2...n) inputs an output Zi of an exponential synthesis function operating device received from the sender and values b_i, P stored in secret to the operator 51 and numerals Y_{n+1} and P obtained from a public table 16 from its output are inputted to as synthesis multiplier 52. Thus, Equation I is satisfied. In such a procedure, the sender qualifies the destination and each destination (i) qualifies the sender because the public list registration information of the sender is used.



⑲日本国特許庁(JP)　特許出願公開

⑫公開特許公報(A)　昭61－63128

⑤1Int.Cl.⁴	識別記号	庁内整理番号	④3公開　昭和61年(1986)4月1日
H 04 L 9/02		Z－7240－5K	

審査請求　未請求　発明の数 1　(全5頁)

⑤4発明の名称　暗号鍵配送方式

②1特　願　昭59－185186

②2出　願　昭59(1984)9月4日

⑦2発明者　岡本　龍明　横須賀市武1丁目2356番地　日本電信電話公社横須賀電気通信研究所内

⑦2発明者　白石　旭　横須賀市武1丁目2356番地　日本電信電話公社横須賀電気通信研究所内

⑦1出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号

⑦4代理人　弁理士　鈴木　誠

明　細　書

1．発明の名称

暗号鍵配送方式

2．特許請求の範囲

(1) 慣用暗号系の暗号鍵を3者以上の間に安全に配送するシステムにおいて、システムで共通に用いられる公開情報を予め定めておくと共に、鍵配送元及び複数の鍵配送先の各者はそれぞれシステムの公開情報に基づき秘密情報及び公開情報を予め生成して公開情報のみ公開簿に登録しておき、鍵配送元が複数の鍵配送先へ鍵を配送する場合、鍵配送元は乱数を生成し、該生成した乱数、各鍵配送先の公開情報及びシステムの公開情報等を用いて各鍵配送先へ転送する情報を生成し、これら情報を受信した各鍵配送先は受信情報と各自が保持する秘密情報等を用いて鍵を得ることを特徴とする暗号鍵配送方式．

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、慣用暗号系の暗号鍵を3者以上に安全に配送する方式に関する．

〔従来技術〕

慣用暗号系の鍵を安全に配送する方式として、離散対数問題の難しさを利用した公開鍵配送方式が提案されている(W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Tran., IT－22, 6, pp644－654, 1976)．しかしながら、この方式は2者間に暗号鍵を配送することはできるが、3者以上に暗号鍵を配送することはできない．

一方、公開鍵配送方式を基本にして、多者に共通鍵を配送できるようにした方式が提案されているが(I. Ingemarsson et. al., "A Conference Key Distribution System", IEEE Tran., IT－28, 5, pp. 714－720, 1982)、この方式は多者間でループ状に通信を行うため同報通信型の暗号鍵配送には適さず、また、暗号鍵共通者の確認のためには別途認証機能が必要となる．

〔発明の目的〕

本発明の目的は、公開鍵配送方式に基づき、同報通信に適した形で3者以上への鍵の配送を行うと共に、配送先、配送元の認証を行うことができる暗号鍵配送方式を提供することにある。

〔発明の構成及び作用〕

本発明は、システムで共通に用いられる公開情報を予め定めておくと共に、鍵配送元及び複数の鍵配送先の各者はそれぞれシステムの公開情報に基づき秘密情報及び公開情報を予め生成し、公開情報のみ公開簿に登録しておき、鍵配送元が複数の鍵配送先へ鍵を配送する場合、鍵配送元は乱数を生成し、その乱数、各鍵配送元の公開情報及びシステムの公開情報等を用いて指数合同関数演算等より各鍵配送先へ転送する情報を生成し、これら情報を受信した各鍵配送先は受信情報と各自が保持する秘密情報等を用いて指数合同関数演算等により鍵を得ることを特徴とする。以下、図面により本発明の内容を詳述する。

まず、システム内で共通に用いられる公開情報としてX，Pを定める。X，Pは次の条件を満たす整数とする。

(i) $1 \leq X \leq P-1$

(ii) Pは素数でかつ(P－1)／2も素数

次に、第1図に示すように、鍵配送元、鍵配送先の各者i(i＝1，2，…，n)は、乱数発生器11、最大公約数演算器12、比較器13より、次式

$$1 \leq a_i \leq P-1 \tag{1}$$

$$GCD(a_i, P-1) = 1 \tag{2}$$

ここで、GCD(X，Y)はX，Yの最大公約数の関係を満足する整数a_iを生成し、それを用いて合同逆数演算器14、指数合同関数演算器15より、次式

$$a_i \cdot b_i \equiv 1 \pmod{P-1} \tag{3}$$

$$Y_i \equiv X^{a_i} \pmod{P} \tag{4}$$

の関係を満足する整数b_i，Y_iを生成し、Y_iを公開情報として公開簿16に登録し、a_i，b_iを秘密に保持する。

次に、配送元が配送先i(i＝1，2，…，n)へ共通鍵を配送するものとする。

まず、第2図で示すように配送元は、乱数γ(1≦γ≦P－1)を乱数発生器21により生成し、公開簿16より得たY_i(i＝1，2，…，n)及びγをPと共に指数合同関数演算器22に入力することにより、次式

$$Z_i \equiv Y_i^{\gamma} \pmod{P} \tag{5}$$

を満足するZ_iを生成し、配送先iへ送付する。また、X，γ，Pを指数合同関数演算器23に入力することにより、配送先iと共通に保持する(つまり、配送先iへ配送したことになる)暗号鍵Kを生成する。つまり、

$$K \equiv X^{\gamma} \pmod{P} \tag{6}$$

次に、第3図で示すように、配送先i(i＝1，2，…n)では、配送元より受け取ったZ_iと秘密に保持するb_i，及びPを指数合同関数演算器30に入力することにより、配送された暗号鍵Kを生成することができ、配送元及び配送先i(i＝1，…，n)の(n＋1)者の間で共通の暗号鍵Kを配送することができたことになる。つまり、

$$K \equiv Z_i^{b_i} \pmod{P} \tag{7}$$

また、以上の配送手順において、配送元は配送先の公開簿登録情報を用いるため、配送元は配送先に対する認証を行ったことになる。つまり、正しいi(i＝1，2，…n)以外の者はKを生成できないため、配送元が鍵配送を意図した者以外へ鍵が配送されることはない。

次に、配送元が配送先を認証するだけでなく、配送先が配送元を認証する方式を示す。

まず、第4図で示すように、配送元(n＋1)は乱数γ(1≦γ≦P－1)を乱数発生器41により生成し、秘密に保持するa_{n+1}とγ，P－1を合同減算器42へ入力し、次式

$$t \equiv \gamma - a_{n+1} \pmod{P-1} \tag{8}$$

の関係を満足するtを生成し、さらに公開簿16より得たY_i(i＝1，2，…，n)及びt，Pを指数合同関数演算器43に入力することにより、次式

$$Z_i \equiv Y_i^{t} \pmod{P} \tag{9}$$

を満足するZ_iを生成し、配送先iへ送付する。また、X，γ，Pを指数合同関数演算器44に入

力することにより、式(8)を満足するKを生成する。これは、配送先iと共有する暗号鍵Kである。

次に、第5図で示すように、配送先i（i＝1，2，…，n）では、配送元より受け取ったZiと秘密に保持するbi及びPを指数合同関数演算器51に入力し、その出力と公開簿16より得たYn+1及びPを合同乗算器52へ入力することにより、次式

$$K \equiv Z_i^{b_i} \cdot Y_{n+1} \pmod{P} \qquad (10)$$

を満足するKを得る。つまり、配送元（n＋1）及び配送先i（i＝1，2，…，n）の(n＋1)者の間で共通の暗号鍵Kを配送することができたことになる。

以上の手順においては、配送元（n＋1）は配送先iの認証を行っていると共に、配送先iは配送元（n＋1）の公開簿登録情報を用いるため、配送先iは配送元の認証を行ったことになる。つまり、正しい配送元（n＋1）以外は、式(10)が成立するようなZiを生成できない。

〔発明の効果〕

以上説明したように、本発明によれば、公開鍵配送方式に基づき、一つの配送元より2者以上への配送先へ鍵の配送を行うと共に、配送先、配送元の認証を行うことができる。

従って、本発明は、同報通信で2者以上に鍵を配送する場合に有効である。

4．図面の簡単な説明

第1図は、配送元、配送先の各者による公開情報、秘密情報の生成を示す図、第2図は、配送元が配送先iへの配送情報及び暗号鍵を生成する場合を示す図、第3図は、第2図に対応した配送先iの暗号鍵の生成を示す図、第4図は、配送元（n＋1）が配送先iへの配送情報及び暗号鍵を生成する場合を示す図、第5図は、第4図に対応した配送先iの暗号鍵の生成を示す図である。

11，21，41…乱数発生器、

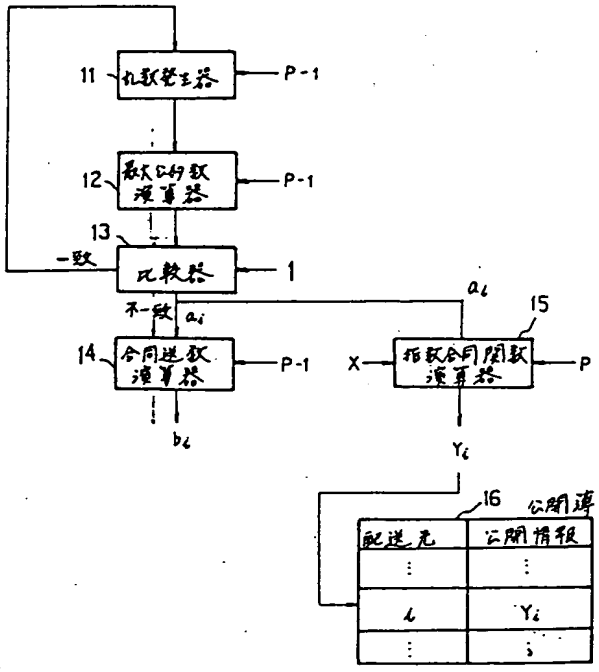
12…最大公約数演算器、　13…比較器、

14…合同逆数演算器、　15，22，23，30，43，44，51…指数合同関数演算器、

16…公開簿、　42…合同減算器、

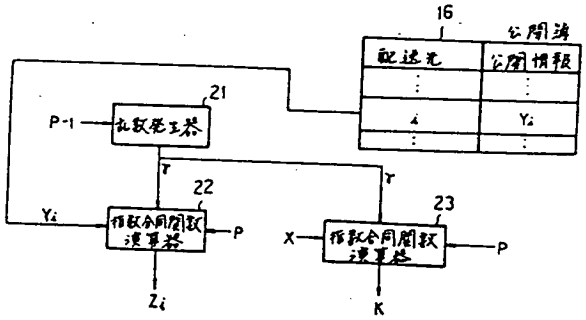
52…合同乗算器。

第　1　図

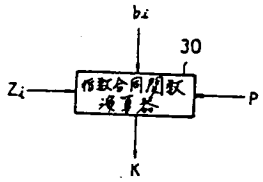


代理人弁理士　鈴　木　　誠

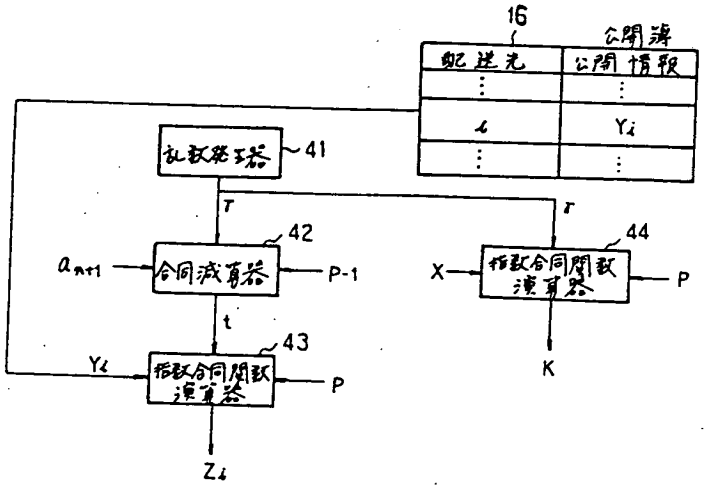
第 2 図


16
公開鍵
配送先
公開情報
Yi
21
礼数発生器
P-1
T
T
22
指数合同関数
演算器
Yi
P
Zi
23
指数合同関数
演算器
X
P
K

第 3 図


bi
30
指数合同関数
演算器
Zi
P
K

第 4 図


16
公開鍵
配送先
公開情報
Yi
礼数発生器
41
T
T
42
合同減算器
am+1
P-1
44
指数合同関数
演算器
X
P
t
43
指数合同関数
演算器
Yi
P
K
Zi

第 5 図